UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,567	02/27/2002	Yanchun Zhao	CA920010020US1	7960

45541 7590 09/18/2008

HOFFMAN WARNICK LLC
75 STATE ST
14TH FLOOR
ALBANY, NY 12207

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
09/18/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOCommunications@hoffmanwarnick.com
PTOCommunications@hoffmanwarnick.com

Office Action Summary	Application No.	Applicant(s)	
	10/084,567	ZHAO ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 June 2008 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-6,8-15,18-22 and 24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 4-6, 8-15, 18-22, 24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on June 18, 2008 has been entered. Claims 1, 2, 4-6, 8-15, 18-22, 24 are pending. Claims 5, 13 are amended by the applicant.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 13, 15, 18-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 13 recites, "Security control apparatus for controlling the security of a network server from unauthorized content contained in a message received from a user of said server, the apparatus comprising: at least one computing device; means for intercepting said message….; means for examining said message....; means for receiving….; a means for retrieving….; means for examining…..; means for determining…..; means for preventing said…..; means for allowing……". The amended claim limitation "at least one computing device" does not clearly provide any functionality of the claimed routines (i.e. it does not show any functional interrelationship, either as part of the stored data or as part of the computing processes performed by the computer). Therefore, claim 13 recites non-statutory subject matter.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, 4-6, 8-15, 18-22, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reshef et al (US Patent No. 6,584,569) in view of Steele et al (US Pub. No. 2003/0191737) and in view of Wagner (US Patent No. 6,085,224).

As per claim 1, Reshef teaches:

examining the messages that flow between a client browser and a server hosting the web application, intercepting said message before any content of said message is processed by said server [Fig. 2A, 2C, col. 5 lines 1-4]; examining said message to determine if it contains one or more unauthorized elements [Fig. 2A, 2C, col. 7 lines 18-67, col. 8 lines 1-12, col. 9 lines 32-51], the examining comprising: receiving an identification of an execution program set to be used to process said message received [col. 9 lines 60-67, col. 10 table 1]; retrieving an identification of all message types associated with said execution program set; examining said message received by said server in relation to said message types associated with said execution program set [col. 10 table 1, lines 26-61, col. 9 lines 32-58].

Reshef teaches intercepting the message (HTTP request/response, which includes an entirety of a string of text based information) before any content of the message is processed by said server [Fig. 2A, col. 5 lines 1-4, Fig. 4, 5] and examining/analyzing the message to detect the unauthorized elements [Fig. 2A, 2C, col. 6 lines 26-67, col. 7 lines 51-67, col. 8 lines 1-34].

Steele teaches: the message (HTTP request/response) includes information entered for constructing a query to access data of the server that includes an entirety of a string of text based information entered by a user into a web page provided by the server directly incorporated therein [Fig. 9A-9C, 10].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Steels with Reshef to realize that the message (HTTP request/response) includes the information entered by the user into the web page, since one would have been motivated to detect security vulnerabilities in a web application [Reshef, col. 2 lines 18-20, 32-34, 44-46].

Wagner teaches:

determining if said message received by said server contains an unauthorized element in relation to the corresponding message type for said message received; if it is determined that said message contains an unauthorized element preventing said message received from being processed by said server; if it is determined that said message does not contain an unauthorized element allowing said message received to be processed by said server [Fig. 1, col. 7 lines 44, col. 15 lines 42-67, col. 16 lines 1-42].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wagner with Reshef and Steels, since one would have been motivated to prevent the execution of interpretive language programs or commands [Wagner, col. 3 lines 45-46].

As per claim 2, the rejection of claim 1 is incorporated and Wagner teaches if it is determined that said message received contains an unauthorized element, preventing said message received from being processed by said server, and causing an error notification to be sent to said user [col. 4 lines 62-67, col. 16 lines 34-47].

As per claim 4, the rejection of claim 1 is incorporated and is rejected for the same reason set forth in the rejection of claim 2 above.

As per claim 5, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 6, the rejection of claim 5 is incorporated and is rejected for the same reason set forth in the rejection of claim 2 above.

As per claim 8, the rejection of claim 5 is incorporated and is rejected for the same reason set forth in the rejection of claim 2 above.

As per claim 9, the rejection of claim 8 is incorporated and further Wagner teaches: if it is determined that said message received does not contain an unauthorized element, allowing said message received to be processed by said serve [Fig. 1, 5, 6].

As per claim 10, the rejection of claim 1 is incorporated and Wagner teaches the message comprising a name value pair [col. 15 lines 51-62, Fig. 3].

As per claim 11, the rejection of claim 1 is incorporated and Wagner teaches said element comprises one or more of the following items: an instruction, a command, a character, a parameter, a token, or a string of any of said previous items [col. 15 lines 51-62, Fig. 3].

As per claim 12, the rejection of claim 11 is incorporated and further Wagner teaches: said element is interpretable as an instruction or command by said server [col. 15 lines 51-62, Fig. 3].

As per claim 13, it is an apparatus claim corresponds to a method claim 1 and is rejected for the same reason set forth in the rejection of claim 1 above.

As per claim 14, the rejection of claim 13 is incorporated and Reshef teaches:

network server comprises an Internet network server and said message is received over the Internet by said server from a user [Fig. 2C].

As per claim 15, the rejection of claim 13 is incorporated and is rejected for the same reason set forth in the rejection of claim 2 above.

As per claims 18 and 19, the rejection of claims 13 and 18 are incorporated and are rejected for the same reason set forth in the rejection of claims 10 and 11 above.

As per claim 20, the rejection of claim 19 is incorporated and is rejected for the same reason set forth in the rejection of claim 12 above.

As per claim 21, the rejection of claim 1 is incorporated and Reshef teaches:
the message types are chosen from the group consisting of: single token; *string;* multiple tokens without keywords: OR, UNION and SEMI-COLON; multiple tokens without keywords: UNION and SEMI-COLON; multiple tokens without keywords: SEMI-COLON; and multiple tokens without restriction [col. 9 lines 40-45, col. 10 table 1].

As per claim 22, the rejection of claim 5 is incorporated and is rejected for the same reason set forth in the rejection of claim 21 above.

As per claim 24, the rejection of claim 1 is incorporated and Steele teaches the query is a database query that includes an entirety of the information entered by the user into a field of the web page [Fig. 9A-9C, 10].

Response to Argument

4. Applicant's arguments filed June 18, 2008 have been fully considered but they are not persuasive.

Regarding to applicant argument that cited references fail to teach or suggest "receiving an identification of an execution program set to be used to process said message received; retrieving an identification of all message types associated with said execution program set", Examiner maintains, since Reshef discloses a proxy for intercepting messages flowing between the client browser and the web server and forwarding them to the scanner for analysis [Fig. 2A]. A parsing engine 16, employed in the crawling state, for parsing HTTP messages and the HTML language encapsulated therein. A database stores the application interface structure and the site's vulnerabilities, the various expert rules. An analysis engine, employed in the analysis stage, for analyzing the application interface structure and applying the various rules based on the parameter. The HTTP and HTML response/message is parsed to extract any path parameters or links encapsulated therein. The response is also parsed to identify other application interface elements such as data parameters [col. 6 lines 41-67, i.e. identifying various message types, col. 9 lines 40-45, Table 1]. The scanner enables the detection and assessment of security vulnerabilities (parameter vulnerabilities, path

vulnerabilities, long-shot vulnerabilities…etc.) based on the various rules (i.e. detection rules, mutation rules, long-shot rules…etc.), as shown in Fig. 1 [col. 7 lines 20-67, col. 8 lines 1-51, Fig. 4, 5]. Therefore, Reshef teaches the claim limitation ""receiving an identification of an execution program set (i.e. various rule set) to be used to process said message received; retrieving an identification of all message types associated with said execution program set (i.e. numeric field, text filed, command, user-selected input options – associated with parameter vulnerability detection rules, scripts directory in the URL, script [command name] – associated with path vulnerability detection rules…etc.). The claimed terms "message types" and "execution program set" is not clearly defined in the claim limitation/language. If applicant believes it differs from the cited one, applicant is reminded that additional modification to clarify the claimed language is necessary for further consideration and distinction from the prior art.

Applicant has amended claim 13 to include the limitations "At least one computing device…." to correct the 35 U.S.C. 101 issue. However, the amended claim has not overcome such deficiency. The amended claim limitation "at least one computing device" does not clearly provide any functionality of the claimed routines (i.e. it does not show any functional interrelationship, either as part of the stored data or as part of the computing processes performed by the computer). Therefore, claim 13 recites non-statutory subject matter.

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP

9/11/08

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135